SYM-AM-16-043

PROCEEDINGS
OF THE
THIRTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

WEDNESDAY SESSIONS VOLUME I

Cybersecurity Figure of Merit

CAPT Brian Erickson, USN, SPAWAR

Published April 30, 2016

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Panel 9. The Operational and Developmental Dimensions of Cybersecurity

Wednesday, May 4, 2016	
3:30 p.m. – 5:00 p.m.	**Chair: Rear Admiral David H. Lewis, USN,** Commander, Space and Naval Warfare Systems Command ***The Cybersecurity Challenge in Acquisition*** Sonia Kaestner, Adjunct Professor, McDonough School of Business, Georgetown University Craig Arndt, Professor, Defense Acquisition University Robin Dillon-Merrill, Professor, Georgetown University ***Improving Security in Software Acquisition and Runtime Integration With Data Retention Specifications*** Daniel Smullen, Research Assistant, Carnegie Mellon University Travis Breaux, Assistant Professor, Carnegie Mellon University ***Cybersecurity Figure of Merit*** CAPT Brian Erickson, USN, SPAWAR

Cybersecurity Figure of Merit

CAPT Brian Erickson, USN—SPAWAR

Executive Summary

Over time, Navy warfighters have grown accustomed to the promise of reliable information technology, based on the experience of more than 30 years of relative peace in this domain. However, inspections, Red Teams, and actual adversaries have shown that this reliance on interconnected technology is not well-founded. In 2012, the Defense Science Board determined that

> nearly every conceivable component within DoD is networked. These networked systems and components are inextricably linked to the Department's ability to project military force and the associated mission assurance. Yet, DoD's networks are built on inherently insecure architectures that are composed of, and increasingly using, foreign parts. While DoD takes great care to secure the use and operation of the "hardware" of its weapon systems, the same level of resource and attention is not spent on the complex network of information technology (IT) systems that are used to support and operate those weapons or critical IT capabilities embedded within them.

In many cases, the Navy bases its strategic and operational plans on the very capabilities a cyber enemy will deny or exploit in war. In an interview with *CHIPS* (2014) magazine, Matt Swartz, Director, Communications and Networks Division Deputy Chief of Naval Operations for Information Dominance (N2/N6) and Navy Task Force Cyber Awakening (TFCA) Lead said,

> Recent real world events and attacks on our Navy systems make clear the cyber threat is increasing. The risk calculus in the cyber domain has changed. Our reliance on connected capabilities has significantly increased the potential consequences of a cyber-attack.

In short, the Department of Defense (DoD) has awakened to *a "reliance vs. reliability"* gap in its networks that the services struggle to measure.

Within the Navy, quality efforts to achieve and measure cybersecurity across multiple strategic, operational, and tactical level commands, program offices, and systems and type commands are often coordinated primarily through assumed adherence to overarching strategic guidance. No single organization has the broad area visibility, resources, and influence to orchestrate these efforts.

Compounding the problem is the DoD's lack of a consistent, widely accepted methodology to measure and clearly and concisely express the operational readiness and programmatic wholeness of Information Technology–based Programs of Record. Existing acquisition metrics do not respond to current operational imperatives and cannot adequately express future risk to mission. *The Navy is unable to measure and express cyber program of record wholeness, platform cyber readiness, and the impact of programmatic and budgetary decisions on cyber readiness, or to quantify the value of specific cybersecurity standards or controls.* Without an accepted means of holistically scoring risk within a system of systems construct, *the Navy cannot consistently shape cybersecurity investment priorities to optimize value in a resource constrained environment*. As a result, the Navy struggles to effectively manage, prioritize, and influence the allocation of resources among competing systems commands and program offices to maximize cyber readiness of the Fleet and to defend those decisions in the planning, programming, and budgeting process.

Cybersecurity Figure of Merit

This paper addresses the lack of a consistent, widely accepted means of measuring current and future cyber risk to mission resulting from acquisition or operational weaknesses in cybersecurity within an Information Technology–based Program of Record through the concept of a Cybersecurity Figure of Merit (CFOM). The objective is to develop a transparent mathematical framework of weighted qualitative and quantitative metrics that expresses the relative effectiveness of an Information Technology–based Program of Record in terms of the completeness and sufficiency of its cybersecurity properties throughout its lifecycle. CFOM can be used to address acquisition readiness for the Milestone Decision Authority as well as impacts of budget decisions on the cybersecurity wholeness of a given program.

CFOM is developed in terms of operational risk as a function of threats, vulnerabilities, and consequences (Defense Science Board, 2012). While CFOM is initially and primarily intended as an acquisition readiness tool, it groups acquisition metrics into operational categories to maintain acquisition's focus on providing future operational capability. As an expression of operational risk, *CFOM predicts future operational risk by measuring a program's long-range budget and spend plan, technology refresh plans, architecture, and sustainment plans through various technical reviews and operational reports.*

CFOM is intended to be a practical application of a large body of theoretical and practical research available on metrics and scoring of cybersecurity. As such, while the authors recognize the mathematical tenets of probability and risk theory, choices between practicality and academic rigor are made in favor of practicality. One of the self-imposed study restraints for initial implementation is that the program must not require new inspections or changes to existing documents and reports to gather the metrics that make up CFOM.

In conclusion, the CFOM framework attempts to provide decision support to both acquisition and operations by enabling greater understanding of

- a program's acquisition readiness in terms of future operational risk throughout its lifecycle.
- the effect of today's budget or technology tradeoffs on future operational risk.
- how technical risk decisions in one part of an enterprise network translate to operational risk at the tactical or operational edge elsewhere.
- how to optimize complex cybersecurity investment combinations to provide the maximum value in terms of operational risk reduction in resource-constrained environments.

Additional work is needed to refine the framework based on real-world data and then to materialize the capability in a software prototype.

References

CHIPS. (2014, October–December). Mr. Matt Swartz talks about task force cyber awakening. Retrieved from http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=5578

Defense Science Board. (2012). *Task Force report: Resilient military systems and the advanced cyber threat*. Retrieved from http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net

Cybersecurity Figure of Merit (CFOM)

04 May 2016

Presented to:

Acquisition Research Symposium – Panel #9

Presented by:

CAPT Brian Erickson
Navy Cybersecurity 58000
Brian.G.Erickson@Navy.Mil

The overall classification of this brief is: UNCLASSIFIED

Why CFOM?

- ▼ The Question:
  - How much does a pound of cyber cost?

- ▼ The Background:
  - Reliance vs Reliability Gap
  - Inability to measure cyber wholeness
  - Inability to shape cyber investments

- ▼ The Methodology
  - CFOM as a predictive measure (mission risk)

Results

- MITRE delivered CFOM technical white paper 30 Sept 15
- Proposed 3 Case Studies
  - CFOM as an Acquisition Readiness Tool
  - CFOM to Optimize Investments
  - CFOM in a System of Systems (CuFOM)
- Identified a potential framework from which to deviate

We are prepared to move forward with CFOM Pilot
Issue: CFOM funding fell below the cut line

Way Forward

- CFOM Phase 2 (pilot)
- CNO funded NPS to develop CFOM Thesis (vignette)
  - Aligned with Dr. Randy Maule and student
  - Focused on a tactical thread via Valiant Shield

Vision

The Navy's C4ISR and Cyber Engineering Authority

Mission

As the Navy's recognized technical leader in C4ISR and Cyber, we provide engineering rigor across the acquisition lifecycle to define, develop, deliver, and sustain well-integrated, interoperable and resilient systems across the Navy